REMARKS

Attached is a terminal disclaimer regarding various related applications filed coincidently with the present application.

The Examiner rejected Claims 14, 16-18, 19, and 21-23 under 35 U.S.C. 102(b) as being anticipated by Venkatesan et al., "Threat-Adaptive Security Policy." Such rejection is now moot in view of the cancellation of such claims hereinabove.

The Examiner continues by rejecting Claims 1, and 5-12 under 35 U.S.C. 103(a) as being unpatentable over "Unified Login with Pluggable Authentication Modules (PAM)" by Samar et al., in view of "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" by Cheng et al. Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove.

Specifically, now claimed in each of the independent claims is the following specific technique for generating the authentication tag:

"wherein a portion of a message associated with the message data is processed using a first function that is utilized at least in part to produce the authentication tag;

wherein said portion of said messagc processed is selected by using a pseudorandom probabilistic function."

Simply nowhere in the prior art cited by the Examiner is there such a combination of features for generating the authentication tag using a function that processes a portion of a message which is selected by using a pseudorandom probabilistic function. A specific prior art showing of such feature in the prior art, or a notice of allowance is respectfully requested.

Still yet, applicant has added numerous dependent claims which are deemed to be novel. In particular, now claimed is:

"wherein said message includes a number of message parts, said message parts are 64-bit words" (see Claim 24);

"means for partitioning said message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function" (see Claim 25);

"wherein said portion of said message processed is selected by:
defining a message selection percentage p; and
using said pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function" (see Claim 26);

"wherein said first function is a keyed hash function" (see Claim 27);

"wherein said first function is one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash al" (see Claim 28); and

"wherein said portion of said message processed is selected by truncating said message" (see Claim 29).

No new matter has been added. A specific prior art showing of such features in the prior art, or a notice of allowance is respectfully requested.

Each of the independent claims is thus deemed allowable, for the reasons set forth hereinabove. Moreover, each of the dependent claims is deemed allowable by virtue of their dependence on the foregoing independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P078/99.042.02).

Respectfully submitted,
Silicon Valley IP Group, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

APPENDIX A

09/621,059 filed on 07/21/2000
09/621,057 filed on 07/21/2000
09/621,056 filed on 07/21/2000
09/621,058 filed on 07/21/2000